Draft Security Contract Language

One critical element that the Department of Education stresses is that IT security must be integrated into an information system *throughout the system's lifecycle*. It is not enough to introduce security controls after a system is already running, or at the end of a system's lifecycle, when it is about to retire. Security needs to be a part of the system from the beginning. The language in this document was created to help ensure that the security requirements for the Department are met by ensuring that contractors know their security responsibilities and know what actions they have to take to meet the Department's security requirements.

This document was created for contract officers as part of an initiative to ensure that security contracting language is consistent for all contracts in the Department. This section provides specifications, tasks, and clauses that can be used in an RFP or SOW to acquire information security features, procedures, and assurances. These specifications, tasks, or clauses are not mandatory, but are intended as a source of general specifications and should be reviewed for applicability to the contract. They are written for different types of acquisitions, including the purchase of COTS products, purchase of integrated systems, development of applications, and other computer-related services.

The specifications, tasks, and clauses are divided into categories. Within each category, there are clauses as well as explanations, considerations, and/or prescriptions about their use. The specifications, tasks, and clauses are printed in Times New Roman font. Explanations, considerations, and prescriptions are in *italics*. These are topics that need to be discussed with security representatives to determine if they need to be included or described in further detail.

If there are any questions, please see the FSA IT Security and Privacy Team.

1. IT Security Compliance

To ensure the confidentiality, integrity, and availability of the Department's business assets the contractor shall comply with the Department's security requirements. The two primary security objectives of the contract are to maintain the security of information when the responsibility for information processing has been outsourced to another organization and having the contractor address in the proposal the risks, security controls and security procedures for facilities, information systems, networks and/or desktop environments as applicable. The Contractor shall comply with and also include the following provisions in any subcontract(s) awarded pursuant to this contract.

In keeping with OMB Circular A-130, Appendix III, security responsibility for a system must be assigned. If the contract calls for information security administration, management, or support, the delineation of responsibilities should be clear, with a government employee retaining ultimate information security program responsibility.

The person responsible for information security for the system is <name>.

The Government authorizes the use of <organization> computer resources (list specific resources if appropriate) for contractor performance of the effort required by the statement of work of this contract.

2. Rules and Regulations

Department of Education systems must adhere to the Federal security requirements detailed in the publications listed below. The following laws, regulations or policies establish minimum requirements for system security.

2.1. Federal Laws and Regulations

- Electronic Communications Privacy Act of 1986, Public Law 99-08, 100 Stat. 1848
- E-Government Act of 2002

- Freedom of Information Act, 5 United States Code 552, Public Law 93-502
- Privacy Act of 1974, 5 United States Code 552a, Public Law 99-08
- Federal Information Security Management Act (FISMA)
- OMB Circulars A-130 Appendix III
- HSPD #7 Critical Infrastructure Protection
- FIPS 46-3 DES
- FIPS 46-3 Triple DES
- FIPS 140-2 Security Requirements for Cryptographic Modules
- FIPS 185 Escrowed Encryption Standard
- FIPS 186-2, Digital Signature Standard (DSS)
- FIPS 197 AES
- FIPS 199 Standards for Security Categorization of Federal Information and Information Systems

2.2. NIST Special Publications

- NIST 800-12 (An Introduction to Computer Security: The NIST Handbook)
- NIST 800-14 (Generally Accepted Principles and Practices for Securing Information Technology Systems)
- NIST 800-16 (Information Technology Security Training Requirements: A Role and Performance-Based Model)
- NIST 800-18 (Guide for Developing Security Plans for Information Technology Systems)
- NIST SP 800-21 (Guideline for Implementing Cryptography in the Federal Government)
- NIST 800-26 (Security Self-Assessment Guide for Information Technology Systems)
- NIST 800-30 (Risk Management Guide)
- NIST 800-34 (Contingency Planning)
- NIST 800-37 (Guidelines for the Security Certification and Accreditation of Federal Information Technology Systems)
- NIST 800-47 (Security Guide for Interconnecting Information Technology Systems)
- NIST 800-53 and 800-53A (Recommended Security Controls for Federal Systems)
- NIST 800-60 (Guide for Mapping Information Systems)

2.3. Departmental of Education Policies and Procedures

- U.S. Department of Education Information Technology Security Policy
- U.S. Department of Education, Information Technology Security Manual, Handbook Number 6
- U.S. Department of Education, Personnel Security-Suitability Program, Handbook Number 11
- U.S. Department of Education, Incident Handling Guide
- U.S. Department of Education Risk Assessment Procedures

- U.S. Department of Education IT Security Configuration Management Procedures Handbook
- U.S. Department of Education Contingency Planning Procedures

Contractors and subcontractors shall also adhere to any new Department policies and procedures that are issued. All of the parties will consider new cost concerns created by implementation of new policies/procedures.

3. Control of Hardware and Software

Only licensed software and in-house developed and authorized code (including government and contractor developed) shall be used on <system name(s)>. Public domain, shareware, or freeware software shall only be installed after prior written approval is obtained from the contracting officer or COTR.

The previous specification is fairly restrictive. The alternatives that follow can be used to modify the specification.

The only hardware and software that shall be used on <system name(s)> is <listed here or specify section>. The contracting officer or COTR must approve all additional hardware and software proposed for use, including upgrades, in advance and in writing.

Alternatives:

1. The contractor shall provide a list of software and hardware changes _____ working days in advance of installing (or other time or performance period).

2. The contractor shall provide test environment analysis for proposed hardware and software and state the security vulnerabilities that were addressed (include other assessment items required) _____ working days in advance of installing.

3. The contractor shall provide proposed hardware and software for testing _____ working days in advance of loading.

4. The contractor shall provide proof of license for new software.

5. The contractor shall maintain a list of hardware, firmware, and software changes throughout the contract. The contractor shall provide this list to the Government (specify time frame and/or at the end of the contract).

If the contractor is using its own software, then the following specification can be used to help protect the Government from buying products developed with stolen software.

The contractor shall provide proof of license for all software used to perform under this contract.

(a) The contractor shall not publish or disclose in any manner, without the contracting officer's written consent, the details of any safeguards either designed or developed by the contractor under this contract or otherwise provided by the Government.

(b) To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of government data, the contractor shall afford the Government access to the contractor's facilities, installation, technical capabilities, operations, documentation, records, and databases.

(c) If new or unanticipated threats or hazards are discovered by either the Government or the contractor, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of the other party.

(d) Under no circumstances is a contractor permitted to make any use of organization computer equipment or supplies for purposes other than performance on this contract.

(e) The following items of government-furnished equipment or software have the following licensing or use restrictions: <provide list>.

(f) The contractor shall not allow its employees to access files that contain employee's passwords.

4. Security requirements

In the proposal, provide solutions for the following:

a) Explain how the availability of services is to be maintained in the event of a disaster;
b) Include a description of each security service that will be provided;
c) Document and adhere to a clear and specified process of change and configuration management;
d) Establish a patch management program in accordance with Department guidelines;
e) Implement incident monitoring and reporting procedures;
f) Document any involvement of the outsourced provider with relevant subcontractors;
g) Create required security documentation, including, but not limited to, Certification and Accreditation plan, System Security Plan, Risk Assessment, Security Test & Evaluation plan, Rules of Behavior, system interconnection agreements, Configuration Management Plan and Contingency Planning documentation;
h) Perform disaster recovery testing for the system at least once a year.

5. Personnel Security Requirements

The contractor agrees to comply with all Department of Education clearance requirements.

Clearance Requirements:
These requirements apply to any contractor or subcontractor staff having access to facilities or systems where ED data is serviced or stored. Requirements for personnel checks imposed by these policies vary commensurate with the sensitivity of the data handled by the employee, and the risk and magnitude of loss or harm associated with the type of position and access the employee requires to complete his/her assigned duties.

The project manager is responsible for identifying by name all contract personnel and the contract labor categories of those requiring access to ED systems. The project manager shall ensure that the required paperwork is properly completed, reviewed for accuracy, and submitted to the Department in a timely manner prior to any contract employee starting to work on the contract.

Contractor staff shall not be in default on any loan made through ED's Title IV programs, including, but not limited to, Federal Stafford, PLUS, SLS, Perkins, and Direct loans.

Personnel assigned to duties under this contract will be subject to investigation by ED. ED's investigation may include, but will not be limited to, the following:

- Checking for defaulted Title IV loans
- Investigation of criminal record
- Checking references on previous employment
- Checking previous security clearances

Procedures:

Contractor and subcontractor personnel must complete and submit the required government forms based on level of clearance and job that is performed. Definitions of the security levels are as follows:

> High Risk (Level 6C) - High risk positions are those positions that have potential for exceptionally serious impact because they involve duties that are especially critical to the ED (for example, project manager and security administrator.)
>
> Moderate Risk (Level 5C) - Moderate risk positions are those positions that have the potential for moderate to serious impact (for example, persons who are responsible for the direction, planning, design, operation, or maintenance

of computer systems.)

Low Risk (Level 1C) - Low risk positions are those positions that require access to the computer systems (for example, application programmers.)

Non-Disclosure Statement Positions (NS)- Depending on job responsibility, and any related limited systems access, a signed copy of the Privacy Act Statement and Declaration for Federal Employment (OF-306) may be the only forms required. Individuals in this category perform duties that are closely monitored and supervised to ensure risk is limited (for example, data entry and documentation specialist.)

Should the COTR NOT require a contractor or subcontractor employee to undergo a background security screening, the following events must occur:

The COTR must be confident that adequate administrative and internal security controls are in place to protect ED assets and information.

Internal System Controls: In the process of defining positions personnel controls such as least privilege, separation of duties and individual accountability are to be established:

- "Least privilege" refers to granting contractor employees only those accesses to facilities and ED system they need to perform their official duties.
- "Separation of duties" refers to dividing roles and responsibilities so that a single individual cannot subvert or control critical processes.
- "Individual accountability" refers to holding individual users responsible for their actions. Behavior on all the systems must be in accordance with established rules.

The required clearance forms are as follows:

FORM	TITLE	COPIES	HIGH (6C)	Moderate (5C)	LOW (1C)	NS
SF-85P	Questionnaire for Public Trust Positions	2*	X	X	X	
OF-306	Declaration for Federal Employment	2*	X	X	X	X
FD-258	Fingerprint Card	1	X	X	X	
	Fair Credit Reporting Act Release	2*	X	X		
NS	Non-Disclosure Statement/Privacy Act	1	X	X	X	X

* Original and one copy

The following steps are required for submitting employee clearance documents:

A. The contractor employee without previous clearance shall complete the required forms, as shown in the above table based upon the defined labor categories. (Note: EVERY employee assigned to the contract in any way must complete the Non-disclosure/Privacy Act Statement and the OF 306).

1) The applicant's labor categories shall be detailed enough to allow the COTR to make a decision that no authorization, need or ability to bypass security controls is involved. The ability and capability to bypass these controls is a major factor in making any security clearance level determination.

2) The COTR will require the applicant to fill out a Non-disclosure/Privacy Act Statement and an OF 306 "Declaration for Federal Employment" form.

B. The contractor employee, with current (non-departmental) or previous clearances (including departmental), who is required to obtain a clearance for employment on this contract must complete a letter on contractor letterhead that provides:

Employee's full name
Date and place of birth
Social Security Number
Type and Level of security clearance
Employer Name (at time of investigation)
Date of investigation
Contract Number
Agency completing the investigation

C. The contractor employee with a current or previous clearance who requires an upgrade due to a change in labor category or system access may be required to provide additional paperwork. The COTR will take the issue to the System Security Officer for a ruling to determine whether any action is necessary.

D. If ED denies a required security clearance, the employee will be ineligible for assignment on this contract. Additionally, ED will check the NSLDS database to ensure that no contractor staff defaults on a Title IV loan while working on the contract.

E. Removal of Project Access:
When employees are removed from contract positions for any reason the contractor shall:

- Revoke all access authorizations and notify the COTR of the removal and the termination date within two working days. If termination is for cause,

immediately revoke system access and follow up by notifying the COTR.
- Retrieve all keys, card keys and badges allowing access to the system facilities.
- Review with the departing employee their obligation to protect system and Departmental Privacy Act data and information.

F. The contractor must notify the SSO if an individual's duties change within the scope of the contract or an individual departs the contract.

6. Control of Information and Data

Any Department information made available in any format shall be used only for carrying out the provisions of this contract. Information contained in such material shall not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract. Disclosure to anyone other than an authorized officer or employee of the contractor shall require written approval of the contracting officer (or contracting officer's technical representative [COTR]).

Any Department information shall be accounted for upon receipt and properly stored before, during and after processing. In addition, all related output shall be given the same level of protection as required for the source material.

If it is necessary to disclose Department information to perform under the contract, the contractor shall request written authorization from the contracting officer (or COTR) to make such necessary disclosure.

The contractor shall ensure that sensitive information shall not be released outside the control of the organization, including release for maintenance or replacement purposes, without the written consent of the contracting officer or COTR.

Should the contractor or one of their employees make any unauthorized disclosure(s) of confidential information, the terms of the Default clause (FAR 52.249-8), incorporated herein by reference, may be invoked, and the contractor will be considered to be in breach of this contract.

7. Contract Performance

The contractor shall provide personnel for a security control/review group, as needed. This group will address security problems, help provide for the maintenance of certification or accreditation under the control of the system security officer, report security problems, and make security recommendations.

8. Information Security Training and Awareness

The contractor shall, at a minimum, certify that all contractor personnel involved in the management, use, and operation of the system(s) who perform work under the subject effort shall have received and will continue to receive annual security and privacy training appropriate to their assignment as defined in NIST SP 800-50, Building an Information Technology Security Awareness and Training Program. Contractors will also complete specialized security training by job function at least annually. Certification of this training shall be provided to the contracting officer no later than <time period> after the training has occurred.

9. Physical Security

If work will be performed at the contractor location, the following section applies.

The contractor shall provide physical security for <list components or systems> other than those in organization-controlled space and for information being transmitted across <list networks>. Physical security measures to be implemented include protecting the following:

- Location (e.g., access to hardware, software, and data)
- Hardware
- Software and data.

The contractor shall identify <name of system or components> equipment that will be in nonDepartment-controlled areas. Methods for physically protecting these systems shall be provided by the Contractor. The protection shall be against damage, unauthorized access, alteration, modification, and destruction, whether by act of nature, accident, or intrusion.

10. Identification and Authentication

The system shall:

- Include a mechanism to require users to uniquely identify themselves to the system before beginning to perform any other actions
- Be able to maintain authentication data that includes information for verifying the claimed identity of individual users (e.g., passwords)
- Protect authentication data so that any unauthorized user cannot access it
- Be able to enforce individual accountability by providing the capability to uniquely identify each individual computer system user
- Raise alarms when attempts are made to guess the authentication data either inadvertently or deliberately).

11. Access Control

The system shall use identification and authorization data to determine user access to information. The system shall be able to define and control access between subjects and

objects in the computer system. The enforcement mechanism (e.g., self/group public controls, access control lists, and roles) shall allow users to specify and control sharing of those objects by other users, or defined groups of users, or by both, and shall provide controls to limit propagation of access rights. These access controls shall be capable of including or excluding access to the granularity of a single user. Access permission to an object by users not already possessing access permission shall be assigned only by authorized users.

12. Testing

Testing shall be conducted on the system before it goes into production. The testing shall occur in a shadow environment/one that is like what the production environment will be, and will be included as a line item in the system life cycle project plan.

13. Auditing

A government management official should be responsible for selecting which events have the potential to be audited and, after system acquisition, which events are recorded in the audit trail. The official must also specify how long audit information is to be retained and on what media.

The system shall be able to create, maintain, and protect from modification or unauthorized access or destruction of an audit trail of accesses to the objects it protects. The audit data shall be protected so that read access to it is limited to those who are authorized.

The system shall be able to record the following types of events: use of identification and authentication mechanisms, introduction of objects into a user's address space (e.g., file open, program initiation), deletion of objects, and actions taken by computer operators and system administrators and/or system security officers and other security relevant events. The system shall also be able to audit any override of human-readable output markings.

This list should be modified to include only those data elements relevant to the system function and environment.

For each recorded event, the audit record shall be able to identify the date and time of the event, user, type of event, and success or failure of the event. For identification and authentication events, the origin of request (e.g., terminal ID) shall be included in the audit record. For events that introduce an object into a user's address space and for object deletion events, the audit record shall include the name of the object and the object's label. The system administrator shall be able to selectively audit the actions of any one or more users based on individual identity and/or object label.

The audit system should raise alarms whenever a threshold is reached with respect to an auditing system resource (disk space in audit log volume) or when auditing has been turned off (either inadvertently or deliberately).

The Contractor will also allow the right of audit and assessment including but not limited to site visits, scanning, penetration testing, interviews by federal agencies, the Department and the Department's contractors.

14. Closeout/Disposal

The contractor certifies that the data processed during the performance of this contract shall be purged and sanitized from all data storage components of its computer facility, and the contractor will retain no output after such time as the contract is completed. If immediate purging of all data storage components is not possible, the contractor certifies that any organization data remaining in any storage component will be safeguarded to prevent unauthorized disclosures.

Government-furnished equipment (GFE), including hardware and software, should be returned in accordance with normal procedures. Special information security considerations include the return of the GFE in usable condition. Returned software shall be certified to be in its original form.

At contract completion or termination, the contractor shall provide a status list of all users and shall note if any users still require access to the system to perform work under another contract. Any group accounts or other means of gaining access to the system also shall be listed, including maintenance accounts and security bypasses.

15. Cryptographic Validations

Cryptographic modules provided by <the system or specific part of the system as defined in the statement of work> shall be validated under the Cryptographic Module Validation Program (CMVP) to conform to FIPS 140-2, Level <insert level>. NIST maintains a list of validated modules at http://csrc.nist.gov/cryptval/. Manufacturers, integrators, and offerors must use BOTH encryption algorithms and modules that have been NIST validated to claim that their products are FIPS compliant. The offeror should be able to identify the validated implementation used in the product by supplying a copy of the validation certificates.

16. Legal Issues

The contracting officer and legal department should be consulted about legal issues. This section addresses some issues that the acquisition initiator may want to discuss with organization acquisition and legal staff.

- *Security Violations – It is possible for computer products to cause security violations, even if the products are functioning correctly. For example, a product*

containing malicious code (i.e., virus or Trojan horse), bypassing operating system controls, or containing undocumented backdoors that bypass security could cause these security violations. Some manufacturers include backdoors so they can assist customers.

- *Allocation of Contractual Risk and Responsibility – The FAR contains general clauses that define the respective responsibilities and allocate risks among the parties to a government contract. However, additional clauses may be needed to fully address specific information security requirements. Such clauses, for example, may address guarantees, warranties, or liquidated damages. The specific wording of such clauses may vary from one solicitation to another because they are a function of the particular need for data integrity, confidentiality, or availability and the nature of the system being protected.*

- *Agencies may wish to consider the use of warranties, liquidated damages, and other clauses in establishing the contractor's information security-related responsibilities in contracts. Such clauses, when properly crafted, will provide incentive to the contractor to ensure that its products and services meet the security requirements of the contract. Such clauses, when poorly drafted or overly broad, can unnecessarily increase contract costs, limit competition, complicate contract administration, and increase litigation risk. These clauses must be prepared in conjunction with existing FAR clauses.*

- Warranties provide a means to require the contractor to fix products after they have been accepted. A warranty is an agreement by the contractor that it will be liable for meeting the contract specifications for a stated period of time after acceptance. (See FAR 46.7 and 52.246-17 through 20.)

- Liquidated damages provide a means for the contractor to compensate the Government for losses that result from contract delays or other problems. The purpose of liquidated damages clauses and other clauses fixing the contractor's performance responsibilities in the information security area is to provide incentive for the contractor to take reasonable steps to ensure that the product does only what it is intended to do and nothing more. For example, the product should be free from malicious code. If the product results in poor security, the contractor can be required to pay for damages. Because the goal is to acquire secure systems, the extent of the liquidated damages clause (or other such clause) should be commensurate with the anticipated risks and damage to the Government. A specific maximum dollar value can be placed on the damages, or other means can be used to limit the contractor's liability. (See FAR 11.5.)

[Note: These are not penalties. If a security violation occurs, but does not result in any loss, the contractor should not be responsible for any liability or liquidated damage.]

The following are examples of integrity statements that may be modified to form a warranty, guarantee, or liquidated damage clause. The examples are not intended to be used together and should be modified for the operating environment. There are no examples of customized enforcement clauses (the specific warranty, guarantee, or

liquidated damage) because they must be developed with the contracting officer and legal counsel. (FAR 52.246-17 through 20 contain FAR standard warranties.)

- The subject product performs in accordance with all specifications, certifications, and representations reflected in the documentation provided in Addendum 1 except as reflected below:

_____

_____

_____

_____

- The installation instructions provided with the subject product, if properly followed, shall result in the creation and modification of only those objects listed below:

_____

_____

_____

- The subject product (hardware or software) shall not interact with any other component (hardware, software, or firmware) of the system onto which it is being installed to perform any function not described in the documentation listed below:

_____

_____

_____

_____

- The instructions provided for removing the subject product from any system onto which it has been properly installed, shall, if properly followed, release back to the system every object used to store the subject product on the system.

- Other than the exceptions listed below, the subject product contains no undocumented functions and no undocumented methods for gaining access to this software or to the computer system on which it is installed. This includes, but is not limited to, master access keys, back doors, or trapdoors.

_____

_____

_____

_____

- The subject product does not interfere or bypass the system security software [[insert name(s) of security software]. The program code performs only request validation

checking and enforces the action that the system security software indicates should be taken. This processing is performed for all users. Any exceptions are listed below:

_____

_____

_____

_____

- *Flaw remediation – Flaw remediation is the process of tracking and correcting security flaws by the contractor.*

  - The contractor shall document the flaw remediation procedures.
  - The contractor shall establish a procedure for accepting and acting upon reports of security flaws and requests for corrections to those flaws.
  - The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the system.
  - The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.
  - The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.
  - The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections, and guidance on corrective actions to the Government.

- The procedures for processing reported security flaws shall ensure that any reported flaws are corrected and the correction issued to the Government.

Caution is required on the sequence of external reporting of security flaws before the corrections are tested. Potential attackers should not be informed of uncorrected security flaws.

- The procedures for processing reported security flaws shall provide safeguards that any corrections to these security flaws do not introduce any new flaws.

- *Government Patents and Ownership – Government patents and ownership of developed software and systems are another important consideration that should be discussed with the contracting officer and legal staff and clearly delineated in RFP and contract text.*